IB/2005/050167

Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

04100230.4

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 04100230.4
Demande no:

Anmeldetag:
Date of filing: 23.01.04
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Intellectual Property & Standards
GmbH
Steindamm 94
20099 Hamburg
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Netzauthentisierung in Heimnetzwerken

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L29/06

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

BESCHREIBUNG

Netzauthentisierung in Heimnetzwerken

Die Erfindung betrifft ein Verfahren zur Netzauthentisierung, insbesondere in Heimnetzwerken, zwischen einem netzinternen und einem netzexternen Gerät.

Im so genannten Consumer-Markt ist die Einfachheit des Gebrauchs (ease of use) ein erheblicher Verkaufsfaktor. Dieses schließt einfache Setup-Prozeduren für Konsumgeräte wie Fernseher, Videorekorder etc. ein. Demzufolge wäre die beste Heimnetzwerk Konfiguration diejenige, die durch automatische Prozeduren, ohne oder mit nur minimaler Benutzerinteraktion erfolgt. Zukünftige Konsumgeräte (CE-Geräte) werden drahtlos miteinander verbunden sein. Die drahtlose Übertragung erstreckt sich jedoch jenseits von Wohnungsgrenzen und kann demzufolge auch in Reichweite der Geräte eines Nachbarn sein. Somit ist sie anfällig für Lauschangriffe und nicht autorisierte Zugriffe. Daher umfasst der Aufbau einer drahtlosen Verbindung zwei weitere entscheidende Gebiete: Mitgliedschaft und Sicherheit. Eine drahtlose Verbindung kann durch automatische Prozeduren eingerichtet werden, jedoch kann ein Gerät ohne jegliche Vorkonfiguration nicht sicher sein, dass es mit dem richtigen Netzwerk verbunden ist, und nicht mit dem eines Nachbarn. Weiterhin kann die Kommunikation, soweit keine Sicherheitsvorkehrungen getroffen wurden, leicht durch ein in der Nähe befindliches Gerät abgehört werden.

Um diese Aufgaben zu lösen, benötigen die Geräte eine gemeinsame Datenbasis, anhand derer sie feststellen können, ob sie zusammengehören, und darüber hinaus gemeinsame sicherheitsrelevante Daten, wie beispielsweise einen kryptographischen Schlüssel, der es ihnen erlaubt, ihre Kommunikation gegen Lauschangriffe zu schützen. Diese gemeinsame Datenbasis muss während des Konfigurationsprozesses installiert werden. Gebräuchliche Verfahren statten alle Geräte mit einer Nutzerschnittstelle zur manuellen Eingabe der Datenbasis aus oder zeigen dem Benutzer verfügbare Optionen, beispielsweise alle sichtbaren drahtlosen Netzwerke, zur Auswahl an. Diese Verfahren haben erhebliche Nachteile hinsichtlich des „ease of use", da die Geräte eine entspre-

chende Benutzerschnittstelle benötigen (Bildschirm, Tastatur, etc.) und die Benutzerführung - insbesondere bei unerfahrenen Benutzern - fehleranfällig ist. Um einen drahtlosen Aufbau durch eine vollautomatische Prozedur zur verwirklichen, ist eine automatische Prozedur erforderlich, die das Mitgliedschaftsproblem löst. Aus der US 2003/0095521 A1 ist ein Netzwerkschema bekannt, bei dem der Zugriff von Kurzstrecken-Netzwerk-Geräten auf WAN/Internet-Netzwerken über eine Art „Zugangsgerät" wie beispielsweise Handy oder PDA erfolgt, welches Verbindung zu beiden Netzwerken hat. Die Authentisierung erfolgt dabei zwischen dem „Zugangsgerät" und dem Terminal des Kurzstrecken-Netzwerks über eine einzugebende PIN. Das Kurzstrecken-Netzwerk kann von einem Dritten, zum Beispiel einem Telekommunikationsprovider verwaltet werden. Hierbei werden die Geräte über den Benutzer, den Verkäufer oder den Provider über eine Vorregistrierung via PIN in das Netzwerk integriert. Dieser Vorgang erfolgt entweder über eine Website oder direkt über ein „Zugangsgerät". Die PIN wird bevorzugt mit dem Gerät geliefert.

Den vorbekannten Methoden gemein ist, dass sie Benutzerinteraktionen in Form von manuellen Eingaben, zum Beispiel einer PIN, erfordern. Derartige Interaktionen setzen entsprechende Nutzerschnittstellen voraus und sind - insbesondere bei unerfahrenen Benutzern - fehleranfällig und erweisen sich insbesondere für diese Benutzergruppe als unkomfortabel. Darüber hinaus ist der Zugriff auf das Kurzstreckennetzwerk bei dem vorbekannten Systemen nicht räumlich definiert, wodurch die Gefahr unautorisierter Zugriffe oder Lauschangriffe nicht ausgeschlossen werden kann.

Vor diesem Hintergrund war es Aufgabe der vorliegenden Erfindung, ein Verfahren zur Netzauthentisierung, insbesondere in Heimnetzwerken bereitzustellen, mit dem eine vollautomatische Integration von drahtlosen Geräten ohne jegliche Benutzereingabe erfolgt und bei dem die Gefahr von unautorisierten Zugriffen oder Lauschangriffen durch räumliche Abgrenzung minimiert wird.

Diese Aufgabe wird dadurch gelöst, dass die Authentisierung zwischen einem netzinternen und einem drahtlosen netzexternen Gerät auf Basis des Vergleichs der Werte beider Geräte erfolgt, die aus deren separaten Messung mindestens eines zuvor definierten Umgebungsparameters resultieren.

Ein neues Gerät, welches mit einer automatischen Prozedur in ein drahtloses Netzwerk integriert werden soll, scannt zunächst das Frequenzspektrum und nimmt Verbindung mit einem Netzinternen Gerät, welches es gefunden hat, beispielsweise einem Accesspoint, auf. Ein derartige Prozedur ist beispielsweise in der IEEE 802.11 standatisiert. Das neue Gerät muss feststellen, ob es mit dem richtigen Partner verbunden ist (und nicht beispielsweise mit einem Gerät des Nachbarn), das netzinterne Gerät seinerseits muss feststellen, ob das neue Gerät berechtigt ist, in das Netzwerk integriert zu werden. Die vorliegende Erfindung schlägt eine Lösung für dieses Problem vor, welche auf der Auswertung der Eigentümlichkeit von Heimnetzwerken basiert. Zwei Geräte prüfen in der folgenden Weise, ob sie zu dem selben Netzwerk gehören: Ein Gerät wählt eine Umgebungsvariable oder ein Set derartiger Variablen (wie beispielsweise Temperatur, Licht etc.) aus, welche eindeutig das Heim und demzufolge das Heimnetzwerk definieren und sendet diese Variablen zu dem anderen Gerät. Anschließend führen beide Geräte eine Messung der entsprechenden Umgebungswerte durch und tauschen die Ergebnisse aus. Stimmen die gemessenen Werte überein, wissen beide Geräte, dass sie zu dem selben Netzwerk gehören und der Konfigurationsprozess kann fortgesetzt werden, wobei das netzinterne Gerät weitere Konfigurationsparameter zu dem neuen Gerät sendet.

Die Aufgabe wird weiterhin durch ein Verfahren gelöst, bei dem die Übermittlung der erforderlichen Konfigurationsdaten von dem netzinternen an das drahtlose netzexterne Gerät verschlüsselt erfolgt und die Verschlüsselung auf den Werten gemessener, zuvor definierter Umgebungsparameter basiert.

In Weiterbildung der Erfindung bestehen die Umgebungsparameter aus vom netzinternen Gerät erzeugten akustischen und/oder optischen Signalen. Hierdurch werden definierte, zeitlich konstante und physikalisch messbare Umgebungseigenschaften erzeugt, wodurch Abweichungen zwischen den Messwerten des netzexternen und des netzinternen Gerätes auf Grund von Zeitverschiebungen der Messvorgänge ausgeschlossen werden.

Bevorzugt werden je Anfrage vom netzinternen Gerät wechselnde Umgebungsparameter definiert. Hierdurch wird verhindert, dass ein externes Gerät die Authentisierung mit wechselnden (z.B. automatisch generierten) Werten wiederholt, bis die entsprechenden Werte getroffen werden. Alternativ oder zusätzlich kann das Authentisierungsverfahren um weitere Mechanismen ergänzt werden, wodurch beispielsweise nach einer vordefinierten Anzahl von Authentisierungsversuchen eines externen Gerätes, weitere Versuche dieses Gerätes für eine bestimmte Zeit automatisch abgelehnt werden.

Vorteilhaft weisen die definierten Umgebungsparameter zeitlich dynamische Werte auf. Hierdurch wird verhindert, dass ein externes Gerät eine erfolgreiche Authentisierung abhört und die übertragenen Daten zu einem späteren Zeitpunkt erneut sendet, um sich selbst zu authentisieren (sog. „replay attack"). Beispielsweise kann das interne Gerät der Kommunikation selbst definierte oder per Zufallsgenerator erzeugte Werte hinzufügen, die vom externen Gerät zusammen mit den Messwerten verschlüsselt zurückgesendet werden.

Grundgedanke der vorliegenden Erfindung ist es, der Natur eines Heimnetzwerkes und der räumlichen Nähe der in diesen verbundene Geräte folgend, dass die in der Umgebung des Netzwerks messbaren Größen zu dem Zeitpunkt, wenn die automatische Konfiguration des Gerätes durchgeführt werden soll, für alle beteiligten Geräte gleich sind. Diese Größen sind jedoch von Geräten außerhalb der betrachteten Umgebung, also außerhalb des Heims, nicht erfassbar.

Andere Weiterbildungen und Ausgestaltungen der Erfindung sind in den übrigen Unteransprüchen angegeben. Ein Ausführungsbeispiel der Erfindung ist in den Zeichnungen dargestellt und wird nachfolgend im Einzelnen beschrieben. Es zeigen:

Figur 1 die Anordnung eines Heimnetzwerks;

Figur 2 das Ablaufdiagramm des erfindungsgemäßen Verfahrens mit Wertabgleich und

Figur 3 das Ablaufdiagramm des erfindungsgemäßen Verfahrens mit Umgebungswertverschlüsselung.

Im Anwendungsbeispiel gemäß Figur 1 ist ein Heimnetzwerk 1 mit internen Geräten 21, 22, 23, 24, 25 angeordnet, auf das ein netzexternes Notebook 3 Zugriff begehrt. Nachdem das Notebook 3 einem Scan verfügbarer drahtloser Netzwerke durchgeführt hat, nimmt es gemäß Figur 2 zur Netzauthentisierung Verbindung zum netzinternen Accesspoint 21 auf, der Mitglied des ausgewählten Netzwerks 1 ist. Der Accesspoint 21 sendet an das Notebook 3 die Umgebungsparameter „Temperatur" und „Akustikfrequenz". Anschließend generiert der Accesspoint 21 ein akustisches Signal mit der Frequenz F_A. Der netzinterne Accesspoint 21 sowie das netzexterne Notebook 3 führen nun eine Messung der Umgebungsparameter „Temperatur" und „Akustikfrequenz" durch, wobei die letztere Messung seitens des Accesspoints 21 entfällt, da diese Frequenz von dem Accesspoint 21 selbst generiert wurde. Nachdem das Notebook 3 seine Messwerte T_N, F_N an den Accesspoint 21 übermittelt hat, vergleicht dieser die erhaltenen Werte mit den selbst ermittelten Werten. Stimmen die gesendeten Werte T_N, F_N mit den eigenen Werten T_A, F_A überein, sendet der Accesspoint 21 die erforderlichen Konfigurationsdaten an das Notebook 3, welches die entsprechende Konfiguration vornimmt und anschließend in das Netzwerk 1 integriert ist. Stimmen die vom Notebook 3 an den Accesspoint 21 übermittelten Werte nicht mit den eigenen Werten überein, so wird dem Notebook 3 der Zugriff auf das Netzwerk 1 verweigert. In diesem Fall wiederholt das Notebook 3 diese Prozedur mit einem Gerät eines anderen verfügbaren Netzwerks.

Dieses Verfahren bietet jedoch noch keinen Ausreichenden Schutz gegen Lauschangriffe. Der Stand der Technik bietet unterschiedliche Verfahren, um die Kommunikation zwischen den Geräten zu sichern. Hierzu verschlüsselt das netzinterne Gerät (Accesspoint 21) die Verbindung mit dem netzexternen Gerät (Notebook 3) mittels bekannter Codierungsverfahren, die auf modernen mathematischen Methoden basieren, und die Möglichkeit bieten, die erforderlichen Schlüssel über die ungeschützte drahtlose Schnittstelle zu übermitteln. Ein solches Verfahren ist beispielsweise die symmetrische Hellman-Verschlüsselung, bei der die Geräte jeweils eine Hälfte ihrer Schlüssel austauschen, oder das asymmetrische private-/public-Schlüsselprinzip, bei dem die Geräte ihre öffentlichen Schlüssel (public key) austauschen. Der Austausch der erforderlichen Schlüssel erfolgt sinnvoller Weise vor der Übermittlung der Umgebungsparameter vom netzinternen Gerät (Accesspoint 21) an das netzexterne Gerät (Notebook 3).

In dem Verfahren gemäß Figur 3 findet kein Abgleich der vom Notebook 3 gemessenen Werte mit den Werten des Accesspoints 21 statt. Der Accesspoint 21 sendet an das Notebook 3 direkt die erforderlichen Konfigurationsdaten, welche jedoch auf Basis der ermittelten Werte „Temperatur T_A“ und „Akustikfrequenz F_A“ kodiert sind. Stimmen die von dem Notebook 3 ermittelten Umgebungswerte T_N, F_N mit denen des Accesspoints 21 überein, so können die übermittelten Konfigurationsdaten entschlüsselt werden und anschließend die Verbindung zum Netzwerk 1 hergestellt werden. Andernfalls können die übermittelten Konfigurationsdaten von dem Notebook 3 nicht entschlüsselt werden, sodass keine Verbindung mit dem Netzwerk 1 aufgebaut werden kann.

Die vorgestellten Verfahren stellen ein neues Paradigma zur Authentifikation eines neuen Gerätes in ein bestehendes Heimnetzwerk dar, welches auf der Interaktion zwischen den Geräten und deren Umgebung basiert. Als sicherheitsrelevante Daten dienen die Messergebnisse einiger definierter Umgebungsvariablen, die separat von dem neuen Gerät, welches es zu konfigurieren gilt und einem der bereits in dem Netzwerk registrierten Geräte ermittelt werden. Das bereits registrierte Gerät dient dabei als Authentifizierer.

Geeignete Umgebungsvariablen zur Authentisierung sind beispielsweise auch die akustische Signatur des Raumes oder ein „Fingerabdruck" der momentanen akustischen Umgebung (wie beispielsweise ein laufendes Klimagerät oder laufende Musik). Alternativ kann auch ein Ultraschallsignal vom netzinternen Gerät generiert werden. Weiterhin geeignete Parameter sind

- modulierte Lichtsignale (sichtbar oder infrarot)
- Lufttemperatur
- Luftfeuchtigkeit
- Lichtinensität der Umgebung
- eine (ggf. gewichtete) Mischung mehrerer Parameter.

An dieser Stelle ist anzumerken, dass die zeitgleiche Durchführung der Messungen durch das zu konfigurierende netzexterne Geräte und das netzinterne Gerät Fehlern des Heimnetzwerkes entgegen wirkt, die durch zeitliche Umgebungsveränderungen hervorgerufen werden können.

Der Ansatz der gemeinsamen Umgebungskenntnisse ist auch für die Authentisierung von Geräten in Powerline-Kommunikationsnetzwerken einsetzbar, die auf Grund ihrer internen Verbindung ebenfalls verwundbar sind hinsichtlich Lauschangriffen und nicht autorisierten Zugriffen. Weiterhin ist der Ansatz für die Einrichtung eines Heimnetzwerkes zwischen zwei Geräten geeignet. In diesem Fall ist einem Gerät die Rolle des „netzinternen" und dem anderen die Rolle des „netzexternen" Gerätes zuzuweisen. Auch ist die Möglichkeit eines Gastzugriffs ermöglicht. Darüber hinaus ist das vorgestellte Verfahren auch in ad-hoc-Netzwerken einsetzbar, welche beispielsweise zwischen willkürlichen Geräten ohne Zugriff auf Infrastruktur und ohne vorher ausgetauschte Schlüssel gebildet werden. In jedem Fall ist sicherzustellen, dass keine unbefugten Geräte sich in derselben Umgebung befinden und unbefugt die Umweltparameter-Prozedur zur Authentisierung durchführen können.

BEZUGSZEICHENLISTE

1	Netzwerk
2	netzinterne Geräte
3	netzexterne Geräte
21 bis 25	netzinternes Gerät

PATENTANSPRÜCHE

1. Verfahren zur Netzauthentisierung, insbesondere in Heimnetzwerken, zwischen einem netzinternen Gerät (21 bis 25) und einem drahtlosen netzexternen Gerät (3), wobei die Authentisierung auf Basis des Vergleichs der Werte beider Geräte erfolgt, die aus deren separaten Messung mindestens eines zuvor definierten Umgebungsparameters resultieren.

2. Verfahren zur Netzauthentisierung, insbesondere in Heimnetzwerken, zwischen einem netzinternen Gerät (21 bis 25) und einem drahtlosen netzexternen Gerät (3), wobei die Übermittlung der erforderlichen Konfigurationsdaten von dem netzinternen Gerät (21 bis 25) an das netzexterne Gerät (3) verschlüsselt erfolgt und die Verschlüsselung auf den Werten gemessener, zuvor definierter Umgebungsparameter basiert.

3. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
dass der Austausch der gemessenen Werte zwischen dem netzinternen Gerät (21 bis 25) und dem netzexternen Gerät (3) verschlüsselt durch zuvor ausgetauschte „public keys" erfolgt.

4. Verfahren nach einem der Ansprüche 1 bis 3,
dadurch gekennzeichnet,
dass die Umgebungsparameter aus vom netzinternen Gerät (21 bis 25) erzeugten akustischen und/oder optischen Signalen besteht.

5. Verfahren nach einem der Ansprüche 1 bis 4,
dadurch gekennzeichnet,
dass je Anfrage vom netzinternen Gerät (21 bis 25) wechselnde Umgebungsparameter definiert werden.

6. Verfahren nach einem der Ansprüche 1 bis 5,
dadurch gekennzeichnet,
dass die definierten Umgebungsparameter zeitlich dynamische Werte aufweisen.

7. Verfahren nach einem der Ansprüche 1 bis 6,
dadurch gekennzeichnet,
dass das netzinterne Gerät (21 bis 25) ein Accesspoint ist.

ZUSAMMENFASSUNG

Netzauthentisierung in Heimnetzwerken

Die Erfindung betrifft ein Verfahren zur Netzauthentisierung, insbesondere in Heimnetzwerken, zwischen einem netzinternen und einem drahtlosen netzexternen Gerät. Die Authentisierung erfolgt auf Basis eines Vergleichs der Werte beider Geräte, die aus deren separaten Messungen mindestens eines zuvor definierten Umgebungsparameters resultieren. Alternativ erfolgt die Authentisierung durch Verschlüsselung von Konfigurationsdaten auf Basis von Werten gemessener, zuvor definierter Umgebungsparameter.

Fig. 1

Fig. 1

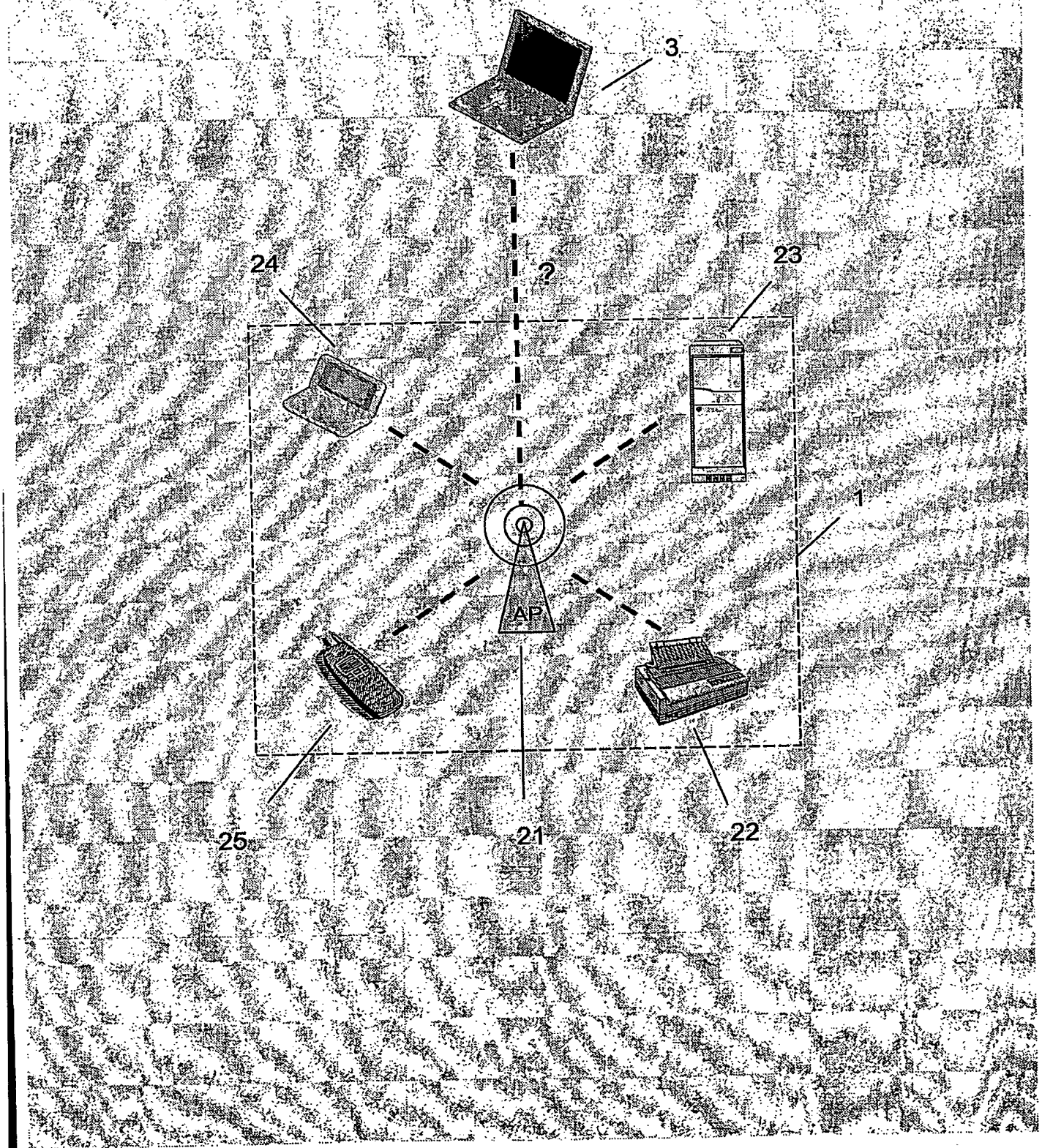


Fig. 2

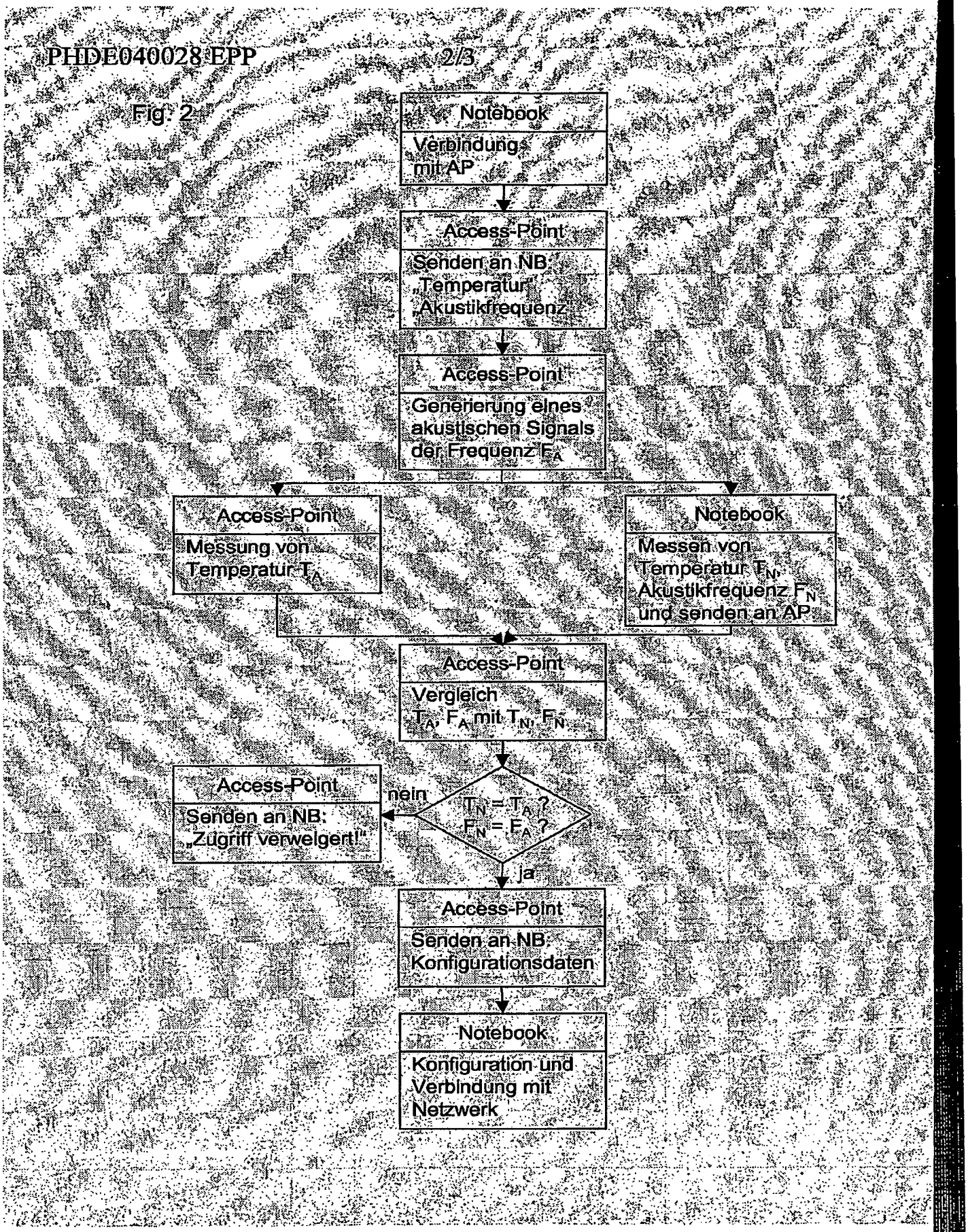
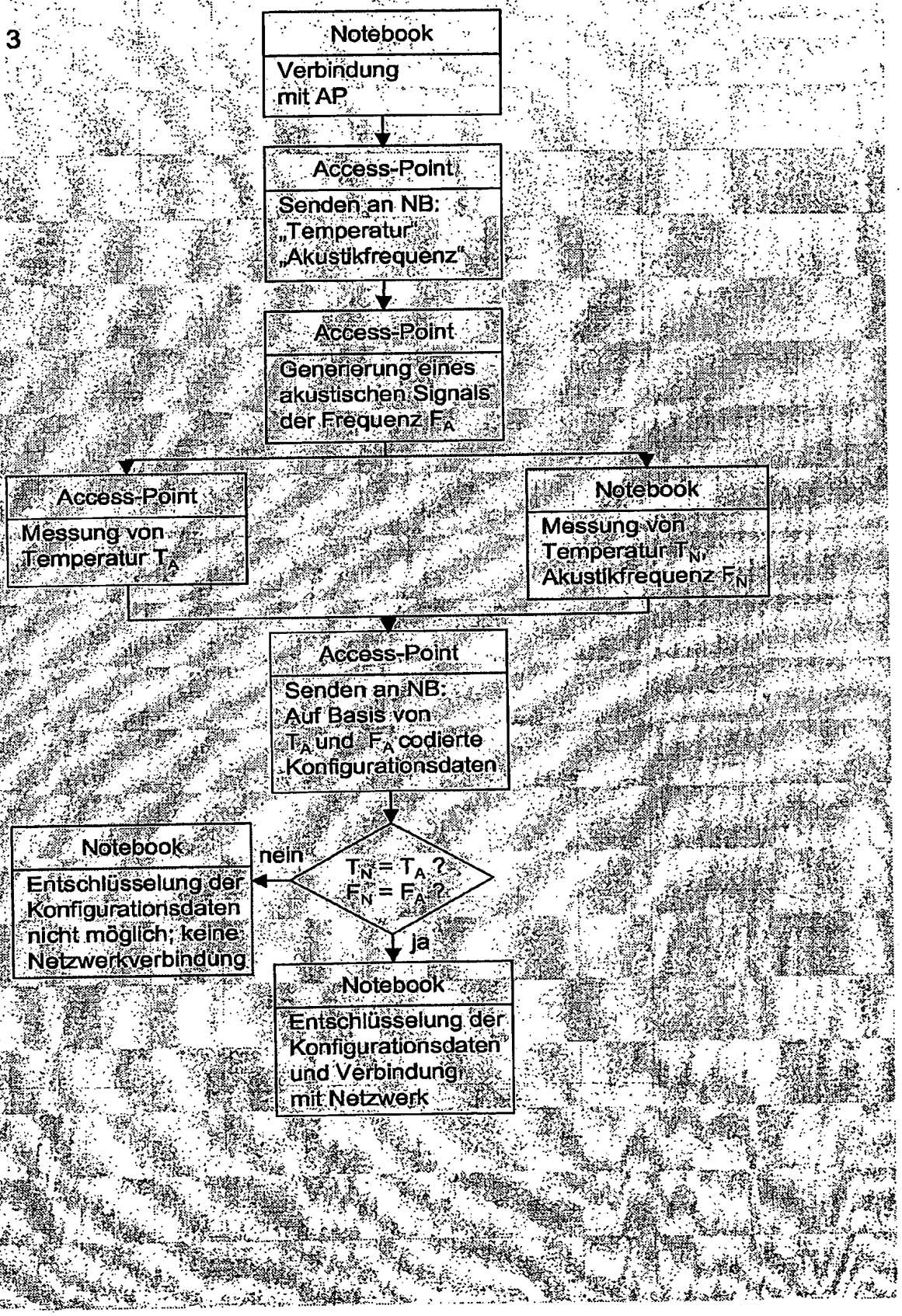

Notebook
Verbindung mit AP
Access-Point
Senden an NB: „Temperatur" „Akustikfrequenz"
Access-Point
Generierung eines akustischen Signals der Frequenz F_A
Access-Point
Messung von Temperatur T_A
Notebook
Messen von Temperatur T_N, Akustikfrequenz F_N und senden an AP
Access-Point
Vergleich T_A, F_A mit T_N, F_N
$T_N = T_A$? $F_N = F_A$?
nein
Access-Point
Senden an NB: „Zugriff verweigert!"
ja
Access-Point
Senden an NB: Konfigurationsdaten
Notebook
Konfiguration und Verbindung mit Netzwerk

Fig. 3


Notebook
Verbindung mit AP
Access-Point
Senden an NB: „Temperatur" „Akustikfrequenz"
Access-Point
Generierung eines akustischen Signals der Frequenz F_A
Access-Point
Messung von Temperatur T_A
Notebook
Messung von Temperatur T_N, Akustikfrequenz F_N
Access-Point
Senden an NB: Auf Basis von T_A und F_A codierte Konfigurationsdaten
$T_N = T_A$? $F_N = F_A$?
nein
Notebook
Entschlüsselung der Konfigurationsdaten nicht möglich; keine Netzwerkverbindung
ja
Notebook
Entschlüsselung der Konfigurationsdaten und Verbindung mit Netzwerk